Understanding India’s Troubling Rise in InternetShutdowns

A Qualitative and Quantitative Analysis

KRIS RUIJGROK
Contents

Acknowledgements .......................................................... 3
About the Author ............................................................ 3
Key Findings ................................................................. 4
Introduction ................................................................. 5
Methods ........................................................................ 6
1. What is an internet shutdown? ........................................ 7
   1.1 Consequences of shutdowns ..................................... 8
   1.2 Causes of shutdowns .............................................. 8
2. How are internet shutdowns issued in India? .................... 11
   2.1 Legal framework .................................................... 11
   2.2 Non-compliance with the new rules ......................... 12
   2.3 Responsible officer politicization ............................ 14
3. Internet shutdowns in India: where, when and how? ........... 16
   3.1 Internet shutdown orders and affected districts .......... 16
   3.2 Internet shutdowns across the country .................... 18
   3.3 Internet shutdown precision .................................... 20
4. Motivations behind India’s internet shutdowns .................. 22
   4.1 Shutdowns to suppress protests and hide human rights abuses 22
   4.2 Internet shutdowns as a little-used tool around elections 24
   4.3 Shutdowns to suppress movements striving for more political autonomy 26
   4.4 Shutdowns in response to communal tensions ............ 26
   4.5 Shutdowns as a tool for BJP state governments .......... 30
   4.6 Shutdowns as an accepted tool for authorized officials to use 31
5. Conclusions ............................................................... 33
6. Recommendations ........................................................ 34
References .................................................................... 35
Acknowledgements

The research behind this report would not have been possible without the funding and support of the Open Technology Fund. The organization’s Information Controls Fellowship provided the ideal platform and network to carry out this unique project. In particular, I would like to thank Adam Lynn for his supervision and support throughout. I am also very much indebted to my host organization, the SFLC.in, and Radhika Jhalani in particular. On multiple occasions, I was lucky to benefit from her diligence, meticulous work, and generous heart. I would moreover like to thank the SFLC.in’s research assistants for their helpful support in Rajasthan and West-Bengal.

In writing the report, I received valuable feedback from Marcus Michaelsen, Ursula Daxecker, Jos Bartman and Marlies Glasius, while John R. Stith did a tremendous job with copy-editing. Thanks to Ura Design for designing the layout. Last but not least, I wish to thank all my interviewees for sharing their time and insights. Our conversations were indispensable for acquiring better insights into the politics behind the shutdowns. All errors and misrepresentations are obviously mine.

About the Author

Dr. Kris Ruijgrok is a political scientist working at the University of Amsterdam. He is interested in the information and communication environments that shape, and are shaped by, authoritarian politics. In 2020, he was an Information Controls Fellow with the Open Technology Fund. Based on his PhD research, including in-depth fieldwork in Malaysia, he published a book with Palgrave Macmillan on the effect of internet use on anti-government protest under authoritarian rule.
Key Findings

1. Internet shutdowns have risen dramatically in India in recent years, particularly in India's Northern and North-Eastern states. With 230 internet shutdowns, the situation is worst in the state (now union territory) of Jammu and Kashmir.

2. The official narrative that internet shutdowns in India have become "increasingly targeted and precise" is only partially supported by evidence as the average duration of shutdowns has increased over time.

3. Rather than addressing a law-and-order problem caused by online fake news and misinformation (as suggested by officials), the use of internet shutdowns in India is an inherently political problem.

4. Understanding the decision-making process behind the issuance of shutdowns requires looking beyond the official regulatory framework given that the specified rules are often not followed and the individuals authorized to order a shutdown are highly susceptible to political manipulation.

5. Internet shutdowns have become a first – instead of a last – resort for officials challenged with communal or social unrest.

6. Shutdowns are issued in India to suppress protest and hide human rights abuses. Their issuance during protests against the Citizenship Amendment Act, primarily in BJP-states, is illustrative of how this tool is used as a means to clamp down on peaceful assembly.

7. Outside of Jammu and Kashmir, internet shutdowns are seldom issued in India during or prior to elections. Most likely, this is because officeholders fear to be punished at the ballot box for issuing an internet shutdown.

8. Regarding shutdowns in Jammu and Kashmir, these instances are primarily utilized in an effort to suppress collective action and hide human rights abuses by security forces. On a more symbolic level, longer shutdowns in the region also serve as a collective punishment for the Kashmiris who strive for greater political recognition.

9. Communal tensions are an important trigger for the internet shutdowns. Rather than erupting spontaneously, these tensions are often deliberately provoked by groups that benefit from communal polarization.

10. Internet shutdowns occur more often in BJP-ruled states than in states where the party is not in power: The probability of an internet shutdown is 3.5 times higher if a district is ruled by a BJP state government.
Introduction

Widely known as the world’s largest democracy, India also holds the dubious distinction of having the highest number of internet shutdowns. In 2020 alone, 115 shutdowns were issued in the country (by contrast Yemen, the nation with the second highest frequency of shutdowns, had only six).\(^1\) Perhaps just as troubling, the frequency of internet shutdowns in India has increased dramatically in recent years. According to the Software Freedom Law Center, India (an Indian NGO working to defend digital rights), there were only six shutdowns in the country in 2014. Every year since 2018, however, there have been at least 100.

When a shutdown takes place in India, government officials usually attempt to justify the measure as either a means to prevent social unrest and ethnic clashes or a move to restore law and order. But critics remain skeptical, pointing to the massive societal, economic, and psychological repercussions wrought by shutdowns, and emphasizing that such an authoritarian practice only serves to limit the free flow of information and silence dissent. Given the importance of this issue and its effect on the world’s second largest populace, this report seeks to provide further insight and a better understanding into India’s internet shutdowns. In particular, who is responsible for issuing these shutdowns? Under what laws are they justified? Where do they occur? How long do they last? And what type of internet do they disable? Ultimately these questions build to the most important one of all: why are shutdowns issued so often in a purportedly democratic state?

Methods

This report draws on fieldwork conducted in the states of Rajasthan and West-Bengal in early 2020. These states were selected for three primary reasons. First, both Rajasthan and West-Bengal faced numerous internet shutdowns between October 2015 and September 2020 (68 and 12, respectively), permitting a more in-depth examination of the decision-making processes behind their issuance. Second, both states were safe enough for meaningful fieldwork to be conducted within their borders (by contrast, Jammu & Kashmir was completely sealed off from the rest of India during the research period). Third, the Software Freedom Law Center, India (SFLC.in) had research assistants in both Rajasthan and West-Bengal who provided logistical and organizational support for the report.

In conducting research, eight interviews were held with government officials who either had the authority to issue an internet shutdown or were close to those who had. Of these eight, three were with the Indian Administrative Service officers (IAS), four were with the Indian Police Service (IPS) and one was with the State Police Service (SPS). In addition, 33 interviews were held with activists, journalists, and academics. All interviewees were given the option to remain anonymous, which some chose to do.

In addition to fieldwork research, this report also relies on quantitative internet shutdown data from the SFLC.in. The Indian government does not formally announce internet shutdowns either before or after they happen, so the SFLC.in’s database is drawn from national and international news reports, as well as individual reports. All individual reports on internet shutdowns are verified through corroborating reports from other sources. In cases of conflicting reports, the SFLC.in verifies its information from primary sources in the affected areas.

---

2 • Software Freedom Law Centre, India. (2020). Internet shutdowns in India. https://internetshutdowns.in/.
1. What is an internet shutdown?

Over the years, nations across the world have used a wide array of measures in their attempts to control cyberspace. Whereas early state controls were mostly “defensive” in nature (focusing on the consistent censoring of content deemed to be sensitive), recent controls such as surveillance, targeted espionage, and counter-information campaigns are more “offensive” in nature. And while the first generation of state controls strove to permanently block information, modern restrictions on content have become more dynamic and case-specific, often permitting restrictions to respond to changing political circumstances. During politically sensitive moments today, such as protests, violence, or elections, blocking states tend to temporarily restrict access to either particular content or, in the case of shutdowns, the entire internet.

For the purposes of this report, an internet shutdown is understood as “a government-imposed disablement of access to the Internet as a whole within a particular locality or localities for any duration of time.”

Notably, this definition only includes government-imposed orders – not shutdowns that are the result of technical failures or those that are imposed by non-state actors. Additionally, this report’s definition of what constitutes a shutdown concerns only blanket access to the internet as a whole, and thus does not include instances where specific content and/or services are disabled. A selective ban on a platform like Facebook or Twitter therefore does not count as an “internet shutdown” for the purposes of this analysis.

---


1.1 Consequences of shutdowns

Existing research on internet shutdowns, in India and beyond, focuses primarily on the consequences of these events (as opposed to their causes). In an effort to dissuade governments from using shutdowns as a tool to control information flows, various studies have demonstrated the severe economic, social, and psychological impacts of these events. Political consequences of internet shutdowns have also been examined, raising doubt over their purported effectiveness from a government point of view. For instance, research has shown that by empowering radical “peripheral leaders,” internet shutdowns in Egypt and Syria actually promoted mobilization rather than stalling it as intended. A similar study also found that shutdowns in Africa were subsequently followed by escalations in pre-existing protests. Refuting an often heard claim by Indian officials that shutdowns are necessary to restore public order, a recent study by Jan Rydzak demonstrated that India’s shutdowns are often followed by violent collective action, which require less communication and coordination than peaceful demonstrations.

1.2 Causes of shutdowns

In contrast to the above examinations of shutdown consequences, far less attention has been devoted to their causes. Nevertheless, some guidance does exist from studies assessing which governments (or parts of the government) are most likely to issue a shutdown and for what reasons. In cases for which attribution has been possible, shutdown orders often derive from central authorities in the highest echelons of power. In Congo and Cameroon for instance, shutdown orders come from institutions close to the presidency, while in Pakistan shutdown orders stem directly from the powerful military. In terms of government type, most governments that issue shutdowns are non-democratic nature.

---

For example, one study found that all of Africa’s internet shutdowns between 2014 and 2019 were issued by either hybrid or authoritarian regimes (not a single African democracy issued a shutdown during that time).¹³

Unpacking the actual reasons for why governments issue internet shutdowns requires making a distinction between the official justifications and, although hard to verify, their true motivation. In the majority of cases, proffered government justifications focus on two often interrelated themes: protecting public order and preventing the spread of misinformation.¹⁴ In the run-up to Benin’s elections for instance, the internet was shut down just after the government issued a warning about online fake news.¹⁵ Similarly, the governments of Pakistan, Cameroon, and Ethiopia often refer to impending threats to national order and security in justifying their shutdowns.¹⁶ Unsurprisingly, advocacy groups tend to respond skeptically towards these justifications, and Access Now’s 2018 #KeepItOn report goes so far as to separate the “official” reasons from the “actual” reasons for internet shutdowns.¹⁷

Most academic observers are also inclined to take the official narratives surrounding shutdowns with a grain of salt, although recent concerns over social media companies’ slow and inadequate handling of online hate speech have made some commentators somewhat more cautious in condemning the issuance of shutdowns.¹⁸

While the true government intentions behind a specific shutdown may differ on a case-by-case basis, three general explanations predominate the existing literature. First and foremost, internet shutdowns are seen as a tool to prevent or contain protests that threaten to challenge the government. Egypt’s 2011 nation-wide internet shutdown amidst the Arab Spring is a prime example, while more recent shutdowns during protests include Congo-Brazzaville (2015), Togo (2017), the DRC (2018), Nicaragua (2018), Chad (2019), Iran (2019), Iraq (2019), Zimbabwe (2019), and Belarus (2020).¹⁹ Second, particularly in Africa, internet shutdowns are employed during contested elections to thwart protests and conceal electoral malpractices.

In 2015-16, half of the elections in Sub-Saharan Africa took place amidst an internet blackout. Similarly, voters in Bangladesh (2018), the DRC (2019), Benin (2019), and Uganda (2021) were also unable to go online on election day. Third, internet shutdowns are also used as a punitive, disciplinary tool for suppressed groups struggling to obtain greater political recognition. Already marginalized groups in Pakistan’s Balochistan, English-speaking Cameroon, China’s Xinjiang, and Myanmar’s Rakhine have all been disconnected from the internet, often for long periods of time, in order to make it more difficult to document their existence or the human rights violations committed against them. Notably, these three core explanations for internet shutdowns are not mutually exclusive, and shutdowns can be issued with any combination of the three in mind.

2. How are internet shutdowns issued in India?

2.1 Legal framework

India’s federal state system consists of 28 states and 9 union territories. In union territories, the national Government of India is responsible for maintaining law order. In states, the elected state government is tasked with that job, passing down orders to key district-level officials in charge of law enforcement: the district magistrate (the DM) and the superintendent of the police (the SP). Until 2017, the DM was authorized under Section 144 of the Criminal Procedure Code (CrPC) to issue an internet shutdown if he/she was of the opinion that such an order was likely to prevent, or tended to prevent, “obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquillity, or a riot or an affray.” Once issued, no mechanism existed to review the legality of the internet shutdown.

In 2017, however, new rules on internet shutdowns were issued under Section 7 of the Indian Telegraph Act, 1885. Under the new Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, the powers for issuing a shutdown due to a "public emergency" (defined as “the prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action”) or in the interest of "public safety" (defined as “the state or condition of freedom from danger or risk for the people at large”) were placed higher up in the administrative system. Under the new rules, each State Home Secretary is now the responsible officer for issuing shutdowns in their state. In union territories, the Union Home Secretary (falling under the Ministry of Home Affairs) is tasked with the job. Emergency orders can still be issued by officers of the rank of Joint Secretary or above, but such orders must be confirmed by one of the abovementioned secretaries within 24 hours. Because DMs are below the level of Joint Secretary, they are no longer technically authorized to issue a shutdown under the new rules. Once authorized, however, the Divisional Commissioner (DC), who usually supervises the functioning of four or five DMs, has the required rank to issue an emergency order.

Although the new rules (including the Supreme Court of India's recent judgement that all shutdown orders need to be published) have brought some minor improvements to the regulatory framework for issuing shutdowns, the overall design and implementation process remains fraught with problems. The terms under which shutdowns may be issued ("public emergency" and "in the interest of public safety") remain overly broad and therefore open to subjective interpretation, and the newly established review mechanisms lack transparency and public oversight. The review committee's meetings take place behind closed doors, no minutes of the meetings are published afterwards, and all of the committee members are part of the executive branch – the same arm of government responsible for issuing the shutdown in the first place.

### 2.2 Non-compliance with the new rules

Further scrutiny of the new framework reveals that even these flawed procedures are often not followed. Shutdown orders are still seldom published, and DMs continue to issue shutdowns under the old rules despite the existence of the more recent and more specific law which should take precedence and preclude them from doing so.
An article in Scroll.in reports that out of the six states that issued a shutdown between late March and early April 2018, only two states followed the new rules (three continued to use the old rules, and the other did not respond to information requests). Responses to Right to Information Act (RTI) requests filed by the SFLC.in reveal that three of the nine shutdown orders from December 2019 were issued under the old rules. Interviews held by the Indian Council for Research on International Economic Relations (ICRIER) with two DMs from Gujarat confirmed that shutdowns were still issued under the old rules, with one DM not even aware that the new rules existed.

Interviews conducted with officials as research for this report indicate similar non-compliance with the new rules. According to a former DM from an Eastern state, the old rules are still used because they are less “burdensome” for officials. In the words of the officer, “It is basically a method by which a lot of rules can be circumvented.”

Although under the new rules only the DC can authorize emergency orders, when asked about who issues the shutdowns in Jaipur the DC of Jaipur responded:

“The police, in the name of the Superintendent, or the DM, makes a request for a shutdown to me. They request my authorization. Then I decide. It always happens this way.”

This claim was later corroborated by two IPS officers and confirmed through observed shutdown orders obtained via RTI requests.

Notably, Jaipur’s DC also said that no review process takes place after he orders a shutdown, though this claim was later contradicted by the Home Secretary of Rajasthan. As per RTI responses received by the SFLC.in, the review committee for the state of Rajasthan failed to perform its role in many cases. Between July 2017 and May 2018, the state government ordered around 40 internet shutdowns, only 11 of which were reviewed as required. Given that many other state governments refuse to respond to RTI requests relating to internet shutdowns, there is no evidence to assume that Rajasthan’s non-compliance with the shutdown rules is an anomaly.


35 Interview with former DM from an Eastern state (IAS), December 1, 2020.


37 Interview with N.R.K Reddy (IPS), February 24, 2020; Interview with A. Shrivastav (IPS), February 26, 2020.


2.3 Responsible officer politicization

Because internet shutdowns are issued by civil servants, it is important to understand how these officials are selected and assigned. All relevant positions under both the old rules (DM) and the new rules (State Secretary and Union Home Secretary) are filled by members of India’s elite civil service, the Indian Administrative Service (IAS). Each year, between 200,000 and 400,000 individuals sit for the civil services exams, out of which only the top 100 or so qualify for the IAS. Once admitted, the new IAS officers follow a two-year training program, after which they are allotted to a state cadre for life, where they usually become a DM after four or five years of service.

IAS officers can be transferred by the state government from one post to another in public interest. Various ministries have formulated guidelines specifying that “the right job should go to the right person, his or her tenure at the post should be at least three to five years,” and that “transfers should be based on adequate grounds.” In reality, however, the transfer system is highly politicized. Loyal civil servants are rewarded by state governments with important positions, whereas officers aligned with opposing political forces often find themselves punished with obscure postings. According to a survey of civil servants in 2010, only 24 percent believed that postings to much-desired positions were made based on merit.

In the same survey, half of the officers reported that undue outside pressure was a significant problem, which is believed to have only increased in recent years. Speaking about the political interferences in India’s civil service, an IPS officer in Rajasthan acknowledged:

“People get transferred too much on the basis of political compulsions, or because they are not aligned to the government in power.”

Such reshuffling is particularly prevalent when a new state government is elected, at which time mass waves of bureaucrats loyal to the new party in power are transferred to important posts.

What does this mean for internet shutdowns? Ultimately, even though IAS officers are technically responsible for issuing them, in reality officers will often look to their political superiors in the state government before ordering a shutdown. Many examples illustrate this politicization. In January 2019 for instance, following instructions from the All India Trinamool Congress (TMC) government of West-Bengal, the internet was made unavailable for those protesting “anti-worker policies” in Kolkata. Allegedly, the TMC leadership felt threatened in its leadership role against Prime Minister Narendra Modi’s Bharatiya Janata Party (BJP) government and gave the police instructions to throttle internet speed at the protest.

---

46 · Interview with N.R.K Reddy (IPS), February 24, 2020.
Similarly, when the passage of the controversial Citizenship Amendment Act (CAA) triggered protests across the country, internet shutdowns were primarily issued by officers in BJP-led states (see section 5.1, below, for more on this topic). While denying their own manipulability, most officials interviewed for this report admitted that internet shutdowns are usually issued “in close cooperation with” and after “consultation of” the state government.49

Given the above, understanding the decision-making process of India’s internet shutdowns goes beyond a simple review of the official regulatory framework. The rules are not always followed, and even when they are, the bureaucratic autonomy of authorized officials is limited. Thus, while the State Home Secretary (in states) and the Union Home Secretary (in UTs) might officially be responsible for the issuing of shutdowns, the state government (for states) and Government of India (GoI) (for UTs), yield significant influence over the ultimate decision. Whenever the political stakes for the state or central government increase, government involvement in the decision-making process becomes more likely and authorized officers will tend to wait for instructions from “above” before proceeding.

49 • Interview with State Police officer North-Eastern state, February 15, 2020; Interview with former DM from an Eastern state (IAS), December 1, 2020.
3. Internet shutdowns in India: where, when, and how?

3.1 Internet shutdown orders and affected districts

Before examining why shutdowns are so frequently issued in India, it is beneficial to explore foundational elements such as when they occur, where they occur, and how long they last. Figure 1, below, displays the recorded shutdown orders per year in India. As the graph demonstrates, a steep increase in the number of shutdown orders occurred from 2016 onwards, reaching peaks of 134 orders in 2018 and 129 orders in 2020. Notably, the SFLC.in data on internet shutdowns used here differs slightly from the Access Now data used in the introduction.

Figure 1: Total number of internet shutdown orders per year in India
There are, however, limitations to the significance of the raw count of shutdown orders given that the geographical coverage of a given order is unspecified. Some shutdown orders are hyper-localized, while others cover entire states (yet regardless, each order counts as one in the above analysis). Likewise, the simple recording of an order by itself does not capture temporal duration, as both long and short shutdowns count as one.

In an effort to provide more insight into these raw numbers, Figure 2, below, displays the number of districts per month that experienced at least one internet shutdown. Under this form of counting, if an internet shutdown order disabled internet access in parts of three districts, all three districts are marked as having faced an internet shutdown in that month. In addition, if the shutdown continues into the following month, the three districts are once again recorded as having experienced a shutdown in the new month.

Similar to Figure 1, Figure 2 displays a steep increase in the number of districts that faced at least one internet shutdown per month, with some striking peaks. In September 2015 for instance, 54 districts faced an internet shutdown when the entire state of Gujarat was cut off from the internet in the wake of the Patidar protests. Similarly, in August 2017, 54 districts were deprived of internet access in the wake of a rape case verdict against a popular spiritual leader. The spikes in 2018 can be traced back to lower caste protests across the country, unrest in the North-East, communal tensions in Uttar Pradesh, and the state government of Rajasthan’s attempt to prevent exam cheating. By far the largest peak came in December 2019 when 87 districts were denied access to the internet amidst protests against the CAA.
### 3.2 Internet shutdowns across the country

Internet shutdowns vary widely across India’s states. Figure 3, below, displays the total number of recorded shutdown orders per state as of September 2020. Jammu and Kashmir (J & K), which was originally a state but has been designated as a union territory since August 2019, has experienced by far most internet shutdowns (230).

Other states where internet shutdowns are relatively common are Rajasthan (68), Uttar Pradesh (29), Haryana (13), Maharashtra (13), and West-Bengal (12). By contrast, there have been no recorded shutdowns in the states of Kerala, Goa, Andhra Pradesh, Chhattisgarh, Himachal Pradesh, Sikkim, and Mizoram.

What is striking about the data in Figure 3 is not only the variation per state, but also the variation across regions. India’s Southern states seldom face internet shutdowns, while they are commonplace in the Northern ones.
To further examine these regional differences, Figures 5 through 9 below display the number of affected districts per month per region (regions are classified as Northern, Central, Southern, Western, Eastern, and North-Eastern). Noteworthy here is not only the high number of affected districts in the Northern states – even when outlier J & K is removed from the analysis – but also the relatively high number of affected districts in the North-Eastern ones. In addition, while districts in Central and Western states have endured relatively few internet shutdowns overall, significant spikes in the number of affected districts occurred during the anti-CAA protests (December 2019, Uttar Pradesh) and the Patidar agitation (end of 2015/beginning of 2016, Gujarat). Throughout the examined time period, districts in India’s Southern and Eastern states were rarely affected by internet shutdowns.

**Figure 4**: Northern States: Chandigarh, Delhi, Haryana, Himachal Pradesh, Jammu and Kashmir, Ladakh, Punjab, & Rajasthan

**Figure 5**: Central States: Uttarakhand, Uttar Pradesh, Madhya Pradesh, & Chhattisgarh

**Figure 6**: Southern States: Tamil Nadu, Kerala, Karnataka, Andhra Pradesh, Telangana, Puducherry, Andaman and Nicobar Islands, & Lakshadweep
3.3 Internet shutdown precision

Pursuant to a December 2019 ruling on internet shutdowns by India’s Supreme Court, responsible officers are now compelled by law to apply "the least intrusive measure" when issuing an order.\(^{50}\) When asked, government officials interviewed for this report claimed they were indeed increasingly making efforts to minimize the negative impacts of internet shutdowns.\(^{51}\) According to an IPS officer from Jaipur:

"The shutdowns have become very targeted and precise. More than a few years back. Only the mobile internet is shut down, and only in a specific area for a short time." \(^{52}\)

Yet an examination of existing data reveals these claims of increased precision are only partially true. Dividing the number of affected districts by the number of shutdown orders provides a rough approximation of the geographic scope of the shutdowns. A review of this analysis corroborates officer claims that the shutdowns have become increasingly targeted in scope.

Figure 10, next page, indicates that whereas in 2012 and 2013 the average number of affected districts per shutdown order was above 10, this number dropped to below three from 2017 onward.

Officer claims of targeted precision are less substantiated, however, with respect to the type of internet that is disabled during shutdowns. It is true that internet shutdowns in India are increasingly targeting only mobile internet (comprising 29% of the shutdowns in 2015, 65% in 2016 and 2017, 94% in 2018, and 92% in 2019).

---

\(^{50}\) Anuradha Bhasin v UoI [WP(C) 1031/2019] and Gulam Nabi Azad v UoI [WP(C) 1164/2019], 129.


\(^{52}\) Interview Malini Agarwal, February 24, 2020.
But nearly 97% of Indian internet users use only mobile networks – giving rise to questions about whether this can indeed be considered “targeted” or more narrow in scope. By “solely” disabling mobile internet, the authorities only spare the 3% of the population that can afford a more expensive wired internet connection – adding a notable socioeconomic dimension to the shutdowns.

Interestingly, additional anecdotal evidence suggests that shutdowns often target private mobile networks (Jio, Airtel, Vodafone), while leaving government-owned BSNL lines untouched. Finally, regarding duration of shutdowns, officer claims of increased targeting are simply unsupported by the data. As Figure 11 demonstrates, the percentage of shutdowns lasting fewer than 24 hours is clearly decreasing over time (though the existence of missing data in this graph, represented by the blue dashed line, must be noted).

Given the above, it is clear that the use of internet shutdowns has increased in India since 2012 – a trend which has operated alongside a rise in regional application differences. Internet shutdowns are commonly issued in India's Northern and North-Eastern states, while Southern and Eastern states remain largely unaffected. Furthermore, the official narrative that internet shutdowns are more targeted and precise than ever is only partially supported by evidence.

---


4. Motivations behind India’s internet shutdowns

Given their rapid increase in issuance, it is important to try to understand the motivations behind India’s shutdowns. What explains their high number? And why do some state governments issue so many, while others issue almost none? Six explanations are set forth below in an attempt to address these complicated questions. Shutdowns in India are issued (1) to suppress protests and hide human rights abuses, (2) as a little-used tool around elections, (3) to suppress movements striving for more political autonomy, (5) in response to communal tensions, (6) as a tool for BJP state governments, and (7) as an accepted tool for authorized officials to use. Notably, the explanations offered below are interrelated and not mutually exclusive from one another.

4.1 Shutdowns to suppress protests and hide human rights abuses

Section 2.2, above, explained how internet shutdowns around the world are frequently issued in an effort to prevent or contain protests. A police officer interviewee serving in a North-Eastern state was surprisingly candid about the fact that this also happens in India. She explained:

“There are sometimes protests that have the risk of stirring up protests in other parts of the state by movements acting in solidarity with the protest. A shutdown can be used to prevent that.”

The internet shutdowns issued during the anti-CAA protests are a prime example of this motivation in practice.

Passed by the central government, the CAA offers fast-track citizenship for non-Muslim migrants from Bangladesh, Afghanistan, and Pakistan. Critics of the legislation contend this path violates India’s secular constitution. Protests against the law escalated in December 2019, after which time internet shutdowns were used to obscure a clampdown on the demonstrators.

The turmoil surrounding the CAA was worst in Uttar Pradesh (UP). Under the state’s BJP government, the following occurred: 12 reported internet shutdowns, 23 killings, thousands of protestors preventively detained, and hundreds of others – including minors – tortured and imprisoned on fabricated charges. Most of the casualties in UP took place on 20 December 2019 (one day after protests had been banned across the state), amidst an internet shutdown in 18 districts.

In the preceding days, internet shutdowns had already been issued – but only in specific cities. The fact that the widespread shutdown in UP took place concurrently with the protest ban, on a day when the authorities could foresee that mass protests were likely to erupt after the weekly gatherings in mosques, indicates the shutdowns were part of a broader plan to crush the ongoing demonstrations.

This indication is reinforced by the level of state repression that was unleashed on protesters resisting the protest ban after the Friday prayers. While the authorities claimed rioters damaging public property were responsible for the violence, multiple fact-finding missions and journalistic reports have refuted this claim. Video-footage showing police personnel destroying CCTV cameras before firing at the protestors also suggests that the shutdowns were part of a larger plan to cover up the crackdown. Similarly in Assam, another BJP-ruled state, the authorities began their clampdown on the anti-CAA protestors just after they issued an internet shutdown and turned off all the street lights.


59 Ibid.


Given that the political power to issue an internet shutdown lies primarily with the state government, it is noteworthy that the fiercest repression against the anti-CAA protesters (including the bulk of the issued internet shutdowns) took place in states led by the BJP. In total, at least 30 people were killed during the anti-CAA protests, most of them Muslims, and all in BJP states: 23 in Uttar Pradesh, 5 in Assam, and 2 in Karnataka. Out of the 19 reported internet shutdowns during the anti-CAA protests, 14 were ordered in BJP-ruled states.

The shutdowns issued during the anti-CAA protests thus provide a clear example of how internet shutdowns can be utilized to aid clampdowns on dissent. Many others exist. Earlier this year, for example, internet shutdowns were issued during a crackdown on peaceful farmer protests in both Haryana and New Delhi. Coincidentally or not, the BJP also rules in Haryana while Delhi’s shutdowns are issued by India’s Union Home Secretary.

4.2 Internet shutdowns as a little-used tool around elections

Although existing research indicates that internet shutdowns are issued during contested elections around the world, in India this is seldom the case. According to Access Now data, J & K was the only Indian state (although now a UT) where internet shutdowns occurred during elections from 2016 to 2019. In 2020, J & K was again the only territory or state to issue an internet shutdown (during its District Development Council Elections in December).

Surprisingly, further analysis reveals that the likelihood of an internet shutdown in India actually decreases in conjunction with elections. Using election data from the Election Commission of India, Figure 12 below shows the probability of an internet shutdown when elections are upcoming within three months. As the graph illustrates, irrespective of whether J & K is part of the analysis, the probability of an internet shutdown decreases when elections draw closer in time. Whereas the probability of an internet shutdown lies below 0.5% when elections are close, it jumps to 2% during normal political times. With outlier J & K excluded from the analysis (graph below), the probability drops to just 0.1% when elections are close compared to 1% during normal political times. The coloured boxes represent the 95% confidence intervals.

### Internet shutdowns & upcoming elections

![Internet shutdowns & upcoming elections](image)

**Figure 12: Internet shutdowns and upcoming elections**

---

The most plausible explanation for this seemingly counterintuitive finding is likely the strong unpopularity of shutdowns amongst the public. It is therefore possible that incumbent governments might fear losing votes if they were to issue an internet shutdown close in time to an election. Still, in the light of other research which has shown that (communal) violence in India tends to increase prior to elections, this finding remains surprising.67

4.3 Shutdowns to suppress movements striving for more political autonomy

As explained in Section 2.2, above, internet shutdowns around the world are often used to suppress domestic movements struggling to obtain greater political recognition and/or autonomous status from the national government. In India, the 230 shutdowns that occurred in J & K fit this category. J & K is home to a long-standing movement for self-determination, including an ongoing armed rebellion. In staunchly resisting this longstanding rebellion, the Indian government has transformed J & K into one of the most militarized zones in the world.68 While the national government claims its military presence is needed to fight Pakistani-funded jihadi terrorism, a recent United Nations report documents widespread and systematic human rights abuses by India’s security forces in the region of Kashmir, including extrajudicial killings, arbitrary detention of protestors, and enforced disappearances.69

Most internet shutdowns in J & K are issued as a precautionary measure on days that are perceived to have the ability to serve as focal points for collective action. National holidays (such as Independence Day or Republic Day), Eid celebrations, and famous militant trials or funerals (or anniversaries thereof) all provide potential opportunities for protest and are therefore often preventively met with an internet shutdown. For this same reason, the authorities disable the internet during and after “encounters” between security forces and armed militants.70 More so than during the armed insurgency in the 1990s, current separatist fighters enjoy relatively high levels of popularity among Kashmir’s population.71 This makes armed encounters risky for the authorities, as large swaths of people often come to the encounter site in support of the militants – often resulting in demonstrations, sloganeering, and stone-throwing intended to provide the militants with an opportunity to escape.72

72 • Ibid.
In light of claims that shutdowns in J & K also serve to hide the security forces’ human rights abuses from public scrutiny, it is telling that J & K’s two longest internet shutdowns coincided with intensified repression. In 2016, in response to the unrest caused by the killing of Burhan Wani (a leader of a separatist armed group), an internet shutdown was issued for 133 days during which time the use of excessive force led to the unlawful killings of between 130 and 145 civilians as well as a high number of injuries. And in August 2019, after the central government unilaterally removed J & K’s special status, an internet shutdown was issued that lasted for 213 days, during which time 33 civilians were reportedly killed, 14 (mostly youth) were tortured, and thousands of Kashmiris were detained without charge.

Similar to the long-lasting shutdowns that occur in other countries, the lengthy shutdowns in J & K could also be seen as collective punishment for the rebellious region. By disconnecting Kashmiris from each other as well as from the outside world for months, those striving for recognition are no longer able to document their existence online. On a more symbolic level, these shutdowns also therefore serve to define the “others” in Indian digital society, demarcating who is included and who is not. For example, when people from J & K are deprived of internet access for months, they can no longer partake in the government’s flagship “Digital India” program (a campaign launched in 2015 to transform India into a digitally empowered society). In addition to their strategic components, the long shutdowns in J & K could therefore also be motivated by something deeper than preventing mobilization and limiting information from getting out.

4.4 Shutdowns in response to communal tensions

Nearly every government official interviewed for this report said “communal tensions” were the primary cause of India’s internet shutdowns. Although it is difficult to pinpoint the true cause of a shutdown, Access Now reporting does indicate that 50 out of the 351 internet shutdowns issued in India from 2016 to 2019 were triggered by “communal violence.” According to the officials, rumours play a key role in the instigation of communal problems, with social media acting as a dangerous catalyst. The shutdowns, in their view, should therefore be understood as a response to the danger posed by the rumour-spreading potential of tools like Facebook and WhatsApp. In the words of an IPS officer from Jaipur: “the spread of online rumours and fake news creates so much problems. It creates so much opportunities for anti-social elements to threaten the harmony in society.”

---

78 Access Now data from #keepiton campaign (2020).
79 Interview with Malini Agarwal (IPS), February 24, 2020.
The DC of Jaipur struck a similar note: “No one likes the shutdowns. No one is in favour. But there is so much fake news in cyberspace.”

The officials responsible for issuing shutdowns thus view communal tensions as a law-and-order problem that can be aggravated and inflamed by social media. As a result, these authorities believe they must respond to such instances with an internet shutdown. What this perspective fails to take into account, however, is that communal tensions (including those that result in shutdowns) do not just spontaneously appear. To the contrary, these events are more often than not anticipated and even “produced.” Nearly every inquiry into a communal riot in India has found evidence of an elaborate planning and mobilization effort. Rather than a law-and-order problem, communal tensions therefore appear (at least partially) to be an inherently political problem that is often deliberately inflamed by groups that seek to benefit from religious polarization. Given this, it is important to determine which political forces are responsible for the communal tensions that lead to internet shutdowns.

Existing and comprehensive literature on communal riots in India indicates that the elites from both Hindu and Muslim communities have actively politicized the “Hindu” and “Muslim” identity, and that once the “communal card” is played by one group, the action reinforces the other group’s communal identity. And yet, numerous studies have shown that Hindu nationalist groups, often closely aligned to the BJP’s mother organization Rashtriya Swayamsevak Sangh (RSS), have deliberately provoked communal strife for economic and political gains. As elections draw near, the BJP benefits from communal incidents that emphasize the importance of “Hindu unity” against the “Muslim threat.” Because the party’s traditional support base lies among higher-caste Hindus, its electoral prospects benefit from communal conflict that pushes lower-caste Hindus to vote along religious rather than caste lines.

In his seminal work, The Production of Hindu-Muslim Violence in Contemporary India, P.R. Brass described the “production process” of communal riots in India. In today’s digital world, the planting of online rumours plays a key role in this process. During Muzaffarnagar’s riots in 2013 (which led to close to 50 deaths and displaced over 40,000 people), RSS affiliates used WhatsApp to circulate “text, audio, and videos—many of them fake—to build a narrative of how Muslims were trapping Hindu girls and killing Hindu boys during riots.” Similarly, during the Bhagalpur riots in Bihar, fake pictures and videos of bleeding Hindu victims were widely shared in pro-BJP Facebook groups.

---

84 - Engineer, A.A. (1989). Communalism and Communal Violence in India. Ajanta Publications (India); Jawahar Nagar, Delhi, 195.
And during communal violence in West-Bengal’s Baduria in 2017, three widely shared pictures – allegedly representing Hindu victims of the riots – were later proven to have come from a Bollywood movie, Bangladesh, and a 2014 murder case.\(^90\)

Predetermined paths of religious processions are another common strategy for creating communal unrest.\(^91\) Under the cloak of performing a religious obligation, certain processions are often “deliberately designed to incite.”\(^92\) By taking routes through Muslim neighbourhoods, the goal of such processions is to provoke a response from the Muslim community by halting before mosques, playing loud music, and hurling insults.\(^93\) After the desired response is provoked, such as the throwing of a stone thrown at the procession, the incident can be portrayed by the organizers as an “illegitimate provocation by the minorities” that is then used to justify violence.\(^94\) Ram Navami processions in particular, which celebrate the birth of Lord Ram, have grown into large-scale events that attract thousands of people, and which are often used as a “pre-text for large pre-mediated riots involving murder, arson and the destruction of property.”\(^95\)

As demonstrated in Table 1, next page, at least 25 internet shutdowns in India were issued before, during, or after a religious procession. This information was compiled for this report by manually reviewing all the news reports used in the SFLC.in database, and seeking additional reports if the information provided was insufficient. The results reveal that both Muslim and Hindu processions trigger shutdowns, though Hindu processions comprise the vast majority. In line with earlier observed trends, most procession-related shutdowns were issued in North-India, and 19 of the 25 were issued in BJP-ruled states (highlighted in orange). Notably, however, the figures in the table likely underestimate the true number of internet shutdowns triggered by religious processions given that news reports do not exist for all of the shutdowns.

---


\(^{93}\) Ibid.


<table>
<thead>
<tr>
<th>No.</th>
<th>District</th>
<th>State</th>
<th>Month</th>
<th>Religious Procession</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Godhra</td>
<td>Gujarat</td>
<td>September 2015</td>
<td>Ganesh Visarjan</td>
</tr>
<tr>
<td>2</td>
<td>Bikaner</td>
<td>Rajasthan</td>
<td>October 2015</td>
<td>Encounter two religious processions, Muharram</td>
</tr>
<tr>
<td>3</td>
<td>Bokaro</td>
<td>Jharkand</td>
<td>April 2016</td>
<td>Ram Navami</td>
</tr>
<tr>
<td>4</td>
<td>Bhilwara</td>
<td>Rajasthan</td>
<td>December 2016</td>
<td>Barawafat, religious procession</td>
</tr>
<tr>
<td>5</td>
<td>Bhilwara</td>
<td>Rajasthan</td>
<td>December 2016</td>
<td>Religious procession</td>
</tr>
<tr>
<td>6</td>
<td>Sikar</td>
<td>Rajasthan</td>
<td>March 2017</td>
<td>Gangaur procession</td>
</tr>
<tr>
<td>7</td>
<td>Chittorgarh</td>
<td>Rajasthan</td>
<td>December 2017</td>
<td>Eid-e-Milad</td>
</tr>
<tr>
<td>8</td>
<td>Bhadrak</td>
<td>Odisha</td>
<td>March 2018</td>
<td>Ram Navami</td>
</tr>
<tr>
<td>9</td>
<td>East Champaran</td>
<td>Bihar</td>
<td>October 2016</td>
<td>Immersion of Durga idols</td>
</tr>
<tr>
<td>10</td>
<td>Nawada</td>
<td>Bihar</td>
<td>September 2017</td>
<td>Taking of Durga idol to nearby village</td>
</tr>
<tr>
<td>11</td>
<td>Bundi</td>
<td>Rajasthan</td>
<td>January 2018</td>
<td>Perform Puja</td>
</tr>
<tr>
<td>12</td>
<td>Paschim Bardhaman</td>
<td>West-Bengal</td>
<td>March 2018</td>
<td>Ram Navami</td>
</tr>
<tr>
<td>13</td>
<td>Bhagalpur</td>
<td>Bihar</td>
<td>March 2018</td>
<td>Hindu New Year procession</td>
</tr>
<tr>
<td>14</td>
<td>Aurangabad</td>
<td>Bihar</td>
<td>March 2018</td>
<td>Ram Navami</td>
</tr>
<tr>
<td>15</td>
<td>Samastipur</td>
<td>Bihar</td>
<td>March 2018</td>
<td>Ram Navami</td>
</tr>
<tr>
<td>16</td>
<td>Tonk</td>
<td>Rajasthan</td>
<td>March 2018</td>
<td>Hindu New Year procession</td>
</tr>
<tr>
<td>17</td>
<td>Bundi</td>
<td>Rajasthan</td>
<td>March 2018</td>
<td>Hanuman Jayanti procession</td>
</tr>
<tr>
<td>18</td>
<td>Pali</td>
<td>Rajasthan</td>
<td>March 2018</td>
<td>Hanuman Jayanti procession</td>
</tr>
<tr>
<td>19</td>
<td>Sitamarhi</td>
<td>Bihar</td>
<td>October 2018</td>
<td>Immersion of Durga Idols</td>
</tr>
<tr>
<td>20</td>
<td>Tonk</td>
<td>Rajasthan</td>
<td>August 2018</td>
<td>Kanwariyas procession</td>
</tr>
<tr>
<td>21</td>
<td>Paschim Bardhaman</td>
<td>West-Bengal</td>
<td>April 2019</td>
<td>Ram Navami</td>
</tr>
<tr>
<td>22</td>
<td>Kendrapara</td>
<td>Odisha</td>
<td>June 2019</td>
<td>Eid al-Fitr</td>
</tr>
<tr>
<td>23</td>
<td>Jaipur</td>
<td>Rajasthan</td>
<td>August 2019</td>
<td>Kanwariyas procession</td>
</tr>
<tr>
<td>24</td>
<td>Jehanabad</td>
<td>Bihar</td>
<td>October 2019</td>
<td>Immersion of Durga Idols</td>
</tr>
<tr>
<td>25</td>
<td>Damoh, Panna, Chhatarpur &amp; Tikamgarh</td>
<td>Madhya Pradesh</td>
<td>November 2019</td>
<td>Eid-e-Milad-un-Nabi</td>
</tr>
</tbody>
</table>

Table 1: Shutdowns triggered by religious processions
4.5 Shutdowns as a tool for BJP state governments

The rise in the use of internet shutdowns in India has also coincided with the rise of the BJP and Prime Minister Modi’s victory in 2014. Sections 5.1 and 5.4 of this report revealed that in BJP-run states, anti-CAA protests were often repressed with internet shutdowns and religious processions were often met with the same. It is worth examining, therefore, whether internet shutdowns occur more often in BJP states.

To address this important inquiry, this report once again relies on information from the Election Commission of India to determine whether the BJP was part of the state government during a month when a shutdown occurred. When such information is insufficient, additional news reports were traced to arrive at the answer. Based on this analysis, from 2012 through the first quarter of 2020, approximately 49% of all district/months were operating under a state government that was at least in-part ruled by the BJP (for reference, the month of government turnover is coded as ruled by a new state government).

Figure 13, below, shows the number of districts per month that were affected by a shutdown in non-BJP (first graph) and BJP states (second graph). The difference is striking. In non-BJP states, the maximum number of affected districts per month remains below 20, the overall trend is stable, and the average number of affected districts per month is 2.7. By contrast, in BJP states there were four months when more than 40 districts were affected. In addition, the trend over time is clearly rising and the average number of affected districts per month is 9.6 (more than 3.5 times greater than in non-BJP states).

Similar results are presented in Figure 14 on the next page. The coloured boxes represent the 95% confidence intervals. During any given month, the predicted probability of an internet shutdown in a BJP district is 3%, while in a non-BJP state it is 0.8%. Removing J & K’s districts from the analysis (second graph) has limited influence on this result (1.7% for BJP against 0.4% for non-BJP). Although the probabilities both decrease slightly, the stark difference between BJP and non-BJP states remains.
Districts in BJP states thus seem to face a much higher risk of being affected by an internet shutdown than those in non-BJP states. This finding is in part supported by the explanations provided in sections 4.1 and 4.4, and also fits the general pattern of observed democratic backsliding under the BJP that has occurred at the national level since the party’s rise to power.\textsuperscript{96} Nonetheless, multiple other factors might explain the identified correlation between BJP rule and internet shutdowns – including the regional differences in India (as shown in section 4.2). The BJP is traditionally less powerful in India’s Southern states, which – coincidentally or not – is also the region where shutdowns seldom occur.

### 4.6 Shutdowns as an accepted tool for authorized officials to use

A final explanation behind India’s rising number of internet shutdowns may simply be their increased acceptance and subsequent overuse by authorities. According to reports, internet shutdowns have become a common response to even the slightest sign of societal tension. In ICRIER’s 2018 report, one administrator was quoted as saying that internet shutdowns had become an “easy measure, not only to control a law-and-order situation, but for the optics.”\textsuperscript{97}

Among officials interviewed for this report, one former DM admitted that an internet shutdown had become a “checklist item” for officials, noting “when there is a communal issue, an internet shutdown is the first thing people do.”\textsuperscript{98}

He further explained: “With every instrument of state power, the first time it is used, is always more difficult, but as more and more upholders of the state and state power start using it, it gains greater acceptability.”\textsuperscript{99}

According to the former DM, issuing a shutdown amidst social unrest has simply become common practice.
The speed with which Indian officials have become apt to issue internet shutdowns was demonstrated in 2016 when thousands of Jats in Haryana vented their anger using widespread violence and destruction of public property. Despite the collapse in public order, the responsible officers were initially “frozen into inaction.” A panel later convened to investigate the officials’ response, reported that the “highest functionaries” in the government failed to show “the kind of guidance, direction and control” that is expected in a crisis of such proportions. To explain the state’s inaction, the report pointed (in line with section 2.3 of this report) to the politicization of the state apparatus, in which officers in situations clearly demanding action waited to respond until they could know what would most please their political masters.

Yet even while the civil service was paralyzed and waiting for instructions from political superiors, an internet shutdown was immediately issued. In fact, the shutdown was issued before the administration made a serious effort to confront and control a looting mob of armed protestors – suggesting that the shutdown was the first, not last, option of recourse.

In addition, the pressure on officials to quickly control riots provides even more incentive to issue a shutdown (officers unable to control a riot within 24 hours are frequently transferred). Combined with an ineffective review process that fails to hold officials accountable for wrongly imposed shutdowns, these expectations contribute to the overuse – and therefore normalization – of internet shutdowns as a tool to quell unrest.

5. Conclusions

Looking to the future, internet shutdowns will continue to be a threat to freedom in India. In the first four months of 2021 alone, no fewer than 18 shutdowns were issued across the country. Despite large public outcries and advocacy campaigns, few signs indicate that the increased use of shutdowns will abate. Understanding this issue and its causes is therefore a critical first step in reversing this problematic trend. Based on qualitative fieldwork conducted in two Indian states, and quantitative data analysis of recorded internet shutdowns across the country, this report has worked to examine and explain internet shutdowns in India. In doing so, six key findings emerged.

First, understanding the decision-making process behind shutdowns requires looking beyond the official rules and procedures to contextualize human action (or inaction). The rules themselves are often not followed, and officials authorized to issue shutdowns are highly susceptible to political manipulation. Of note, state governments yield an especially significant influence over officers tasked with issuing shutdowns.

Second, internet shutdowns have risen dramatically in recent years, particularly in India’s Northern and North-Eastern states. By contrast, shutdowns are rarely issued in India’s Southern states.

Third, the official narrative that internet shutdowns have become increasingly targeted and precise is only partially supported by the evidence. While shutdowns have indeed become more geographically precise, they now last longer than before.

Fourth, internet shutdowns in India are used to thwart protests, hide human rights abuses, and suppress efforts to obtain increased political autonomy. Yet they are not used to manipulate elections (at least outside of J & K).

Fifth, communal tensions that are deliberately provoked serve as an important cause of shutdowns, which occur more often in BJP-ruled states. Overuse of shutdowns has also resulted in their issuance becoming an accepted and commonplace response to social unrest.

Finally, while the Indian authorities present their use of internet shutdowns as a response to a law-and-order problem caused by online fake news and misinformation, evidence collected for this report emphasizes the shutdowns’ political dimensions.
6. Recommendations

In light of the above findings and analysis, six recommendations are offered in an attempt to address India's troubling rise in internet shutdowns.

i. Any sustainable solution to address India's rise in internet shutdowns must take into account the political context and be situated within a broader movement to obtain the protection of civil and political rights.

ii. Officials tasked with issuing shutdowns should be better protected from political interference. As already stated by a Supreme Court Judgement in 2013, there should be a fixed minimum tenure for responsible officers. In addition, civil service boards, composed of senior civil servants, should manage the transfers, postings, rewards, and punishments of such officers.

iii. Prior to issuing a shutdown order, all available alternatives must be exhausted and documented. Authorities should not issue an internet shutdown without first (or at least simultaneously) making a serious effort to control a law-and-order situation on the ground. In addition, the use of counterspeech should be further explored as an alternative to the internet shutdown.

iv. Despite their limitations, the new internet shutdown rules should be the only procedure followed when issuing shutdowns. In line with Indian Supreme Court precedent, the new rules must also be overhauled to increase transparency and public oversight. All shutdown orders should be published, all shutdown orders must specify a time limit, and the review committee must review all shutdown orders within seven working days.

v. The review committee for shutdown orders needs to become completely independent from the executive branch which is responsible for issuing the internet shutdowns.

vi. The review committee's work, including their assessment of the necessity and proportionality of an issued internet shutdown, should be accessible for all citizens.

106 • T. S. R. Subramanian & Ors v UoI & Ors [WP(C) 82/2011][WP(C) 234/2011].
108 • Anuradha Bhasin v UoI [WP(C) 1031/2019] and Gulam Nabi Azad v UoI [WP(C) 1164/2019].
References

Access Now data from #keepiton campaign (2020).


Anuradha Bhasin v UoI [WP(C) 1031/2019] and Gulam Nabi Azad v UoI [WP(C) 1164/2019].


People’s Union for Civil Liberties v. Union of India. AIR 1997 SC 568.


T. S. R. Subramanian & Ors v UoI & Ors [WP(C) 82/2011] [WP(C) 234/2011].


